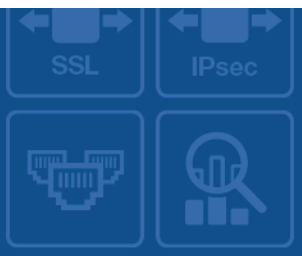
FORTINET
High Performance Network Security

# FortiOS™ Handbook - Security Fabric

VERSION 5.4.1




**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

9/2/2016

FortiOS™ Handbook - Security Fabric

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| Sept 2, 2016 | Initial release |
| | |
| | |
| | |
| | |

# Introduction

This guide explains how to configure your network as a Security Fabric. It contains the following sections:



Because Security Fabric is a new feature in FortiOS and other Fortinet products, it will be developing and expanding as new firmware is released. Please refer back to this document for information about these changes when new firmware is available.

# Overview

This section provides an overview of what a Security Fabric is and how the devices in the fabric work together as a whole. It contains the following topics:



## What is a Security Fabric?

A Security Fabric uses FortiTelemetry to link different security sensors and tools together to collect, coordinate, and respond to malicious behavior anywhere it occurs on your network in real time.

The core of a security fabric is an upstream FortiGate located at the edge of the network, with several internal FortiGates functioning as Internet Segmentation Firewalls (ISFWs). A security fabric can be used to coordinate the behavior of other Fortinet products in your network, including FortiAnalyzer, FortiManager, FortiClient, FortiClient EMS, FortiWeb, FortiSwitch, and FortiAP.

A security fabric ties your network together data to provide visibility and control. The Fortinet Security fabric covers:

- Endpoint client security
- Secure wired, wireless, and VPN access
- Network security
- Data center security (physical and virtual)
- Application (OTS and custom) security
- Cloud security
- Content (email and web) security
- Infrastructure (switching and routing) security

Multiple VDOM support is disabled when security fabric is enabled.

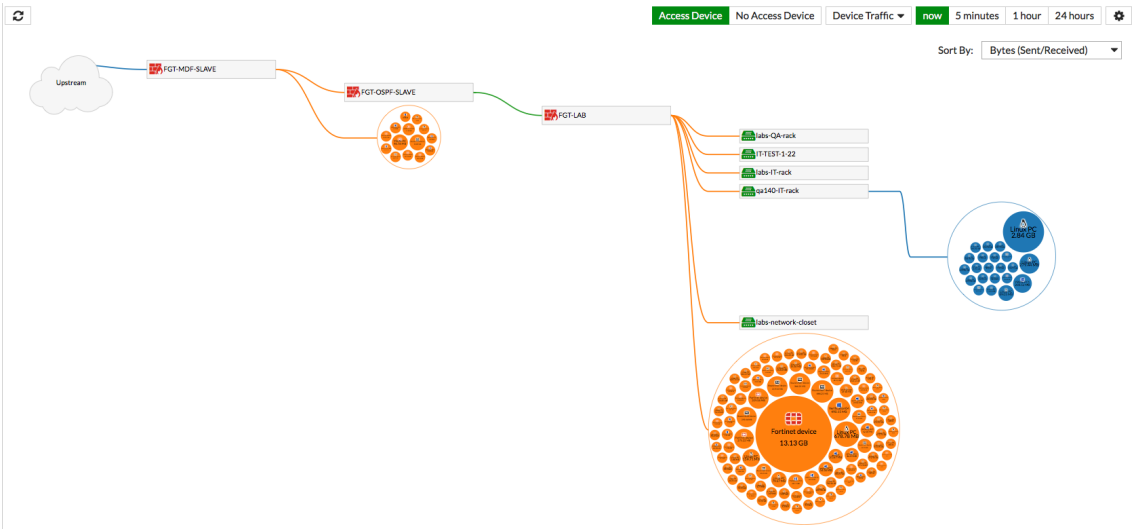
## FortiView

FortiView can be used to view a security fabric's topology. Two different visualizations are available: Physical Topology and Logical Topology.

Both visualizations can be filtered to show four main views: device traffic, device count, device type, or no devices. Finally, like other FortiView pages, the topology can be filtered by time.

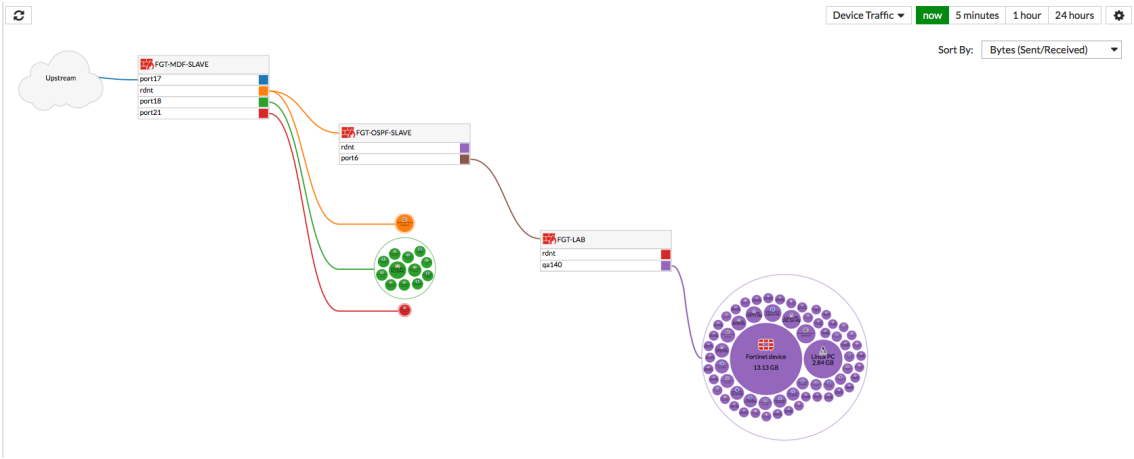
## Physical Topology

Physical Topology shows the devices in the security fabric and which devices are connected. You can select whether or not to view access layer devices in this topology.




## Logical Topology

Logical Topology displays information about network interface (logical or physical) and which interfaces are used to connect devices in the fabric.




# Communication Between Devices

There are two main ways that devices within a security fabric communicate with each other: FortiTelemetry and Routing using OSPF.

## FortiTelemetry

FortiTelemetry is a protocol, similar to the FGCP HA heartbeat, used for communication between the Fortinet products in the security fabric. FortiTelemetry connects devices in a security fabric allowing dynamic status updates between these devices. FortiTelemetry also supports FortiClient On-Net functionality, and monitors and enforces FortiClient protection on user endpoints devices on the network.

FortiTelemetry must be enabled on interfaces that connect Fortinet devices in the security fabric.

## Routing using OSPF

Dynamic routing, most often using OSPF, is recommended for allowing communication among all of the devices in a security fabric. OSPF can be set up relatively easily on all of the FortiGate units in the security fabric from the FortiGate GUI. Since FortiOS fully supports OSPF, no additional routers are required.

For an example OSPF setup for an example security fabric, see Installing internal FortiGates and enabling a security fabric.

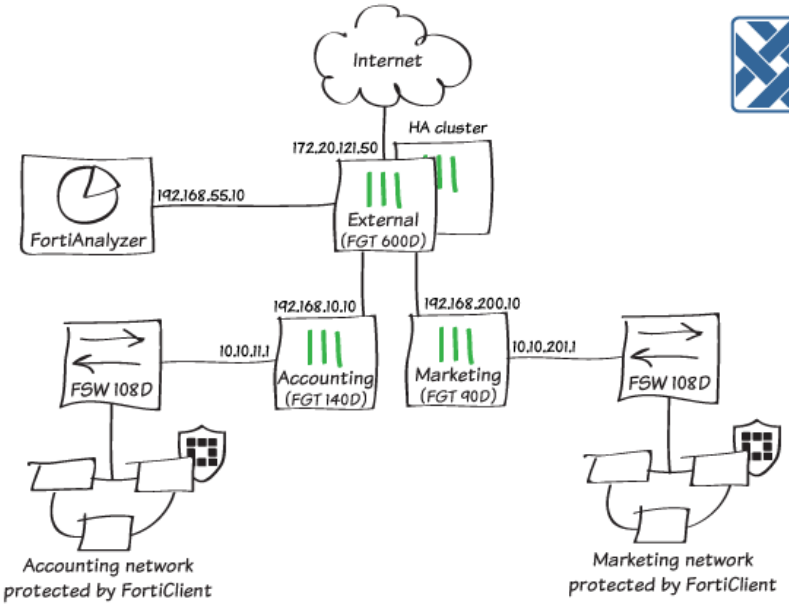
# Firmware Versions

Some features of the Security Fabric are only available in certain firmware versions. The chart below shows the products that have required firmware versions.

| Product | Required Firmware |
|---|---|
| FortiGate | 5.4.1 |
| FortiAnalyzer | 5.4.1 |
| FortiManager | 5.4.1 |
| FortiClient | 5.4.1 |
| FortiSwitch | 3.4.2 and later |
| FortiAP | 5.4.1 |
| FortiSandbox | 2.1.0 and later<br>1.4.0 and later |

For any additional compatibility information, please refer to the Release Notes.

# Example Network




To demonstrate how to configure a security fabric, the Security Fabric collection is available on Fortinet Cookbook website. Currently the Security Fabric collection includes the following recipes:

- Installing a FortiGate in NAT/Route Mode
- Installing internal FortiGates and enabling a security fabric
- Adding FortiAnalyzer to a security fabric
- High Availability with two FortiGates
- Setting up an internal network with a managed FortiSwitch
- Adding endpoint control to a security fabric

This collection will expand over time, so check back to see if anything new has been added.

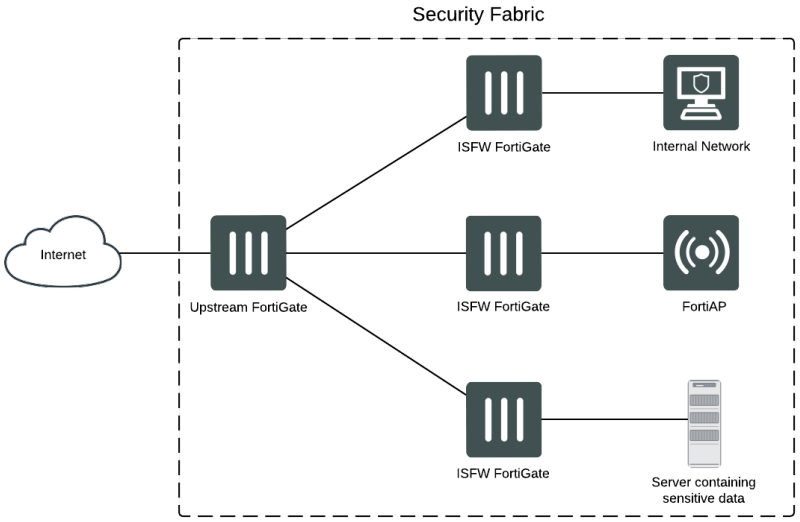
# Core Devices

The following Fortinet products are the key components of a Security Fabric:

- FortiGate
- FortiAnalyzer
- FortiManager
- FortiClient
- FortiClient EMS

## FortiGate

There are two roles a FortiGate can have in a security fabric: Upstream or Internal Segmentation Firewall (ISFW). Both FortiGates work together to provide Distributing security functions.




### Upstream

The upstream FortiGate is the heart of the security fabric. It is located on the edge of the network, connecting the internal devices and networks to the Internet through your ISP.

From the upstream FortiGate, you can view information about the entire security fabric using FortiView.

### Internal Segmentation Firewall (ISFW)

Once an upstream FortiGate has been installed, all other FortiGates in the security fabric act as Internal Segmentation Firewalls (ISFWs).

An ISFW is a firewall that sits at strategic internal points of the internal network, rather than on the network edge. This allows extra security measures to be taken around key network components, such a servers that contain valuable intellectual property.

ISFW FortiGates in a security fabric send traffic and information about their devices to the upstream FortiGate, allowing network visibility.

### Distributing security functions

Security Fabric configurations allow you to distribute security functions to different FortiGates in the security fabric. For example, you may want to implement virus scanning on the External FortiGate but add application control and web filtering to the ISFW FortiGates.

This results in distributed processing between the FortiGates in the Security Fabric; reducing the load on each one. It also allows you to customize the web filtering and application control for the specific needs of the Accounting network as other internal networks may have different application control and web filtering requirements. This configuration may result in threats getting through the External FortiGate which means you should very closely limit access to the network connections between the FortiGates in the Security Fabric.

Another strategy you could choose is to have flow-based inspection on the External FortiGate and proxy-based inspection used by the ISFW FortiGates.

## FortiAnalyzer

Using a FortiAnalyzer in a security fabric allows you to simplify network logging by storing and displaying all log information in one place.

Currently, FortiAnalyzer does not have any security fabric specific features. However, you can configure all of the FortiGates in the security fabric to send log messages to your FortiAnalyzer and use its analysis tools on this data.

To add FortiAnalyzer to a fabric, all FortiGates in the fabric must be able to send logs to the FortiAnalyzer. To do this, go to **Log & Report > Log Settings** and configure **Remote Logging and Archiving** to send logs to the FortiAnalyzer.

## FortiManager

Using a FortiManager in a security fabric allows you to simplify network management by centralizing management access in a single device.

Currently, FortiManager does not have any security fabric specific features.

To add FortiManager to a fabric, all FortiGates in the fabric must be able to send logs to the FortiAnalyzer. To do this, go to **Log & Report > Log Settings** and configure **Remote Logging and Archiving** to send logs to the FortiManager.

## FortiClient

FortiClient is used to add endpoint control to devices located within a security fabric. This is done by creating a FortiClient Profile that only allows traffic from compliant devices to flow through the FortiGate.

In a security fabric, FortiClient profiles are applied by the first FortiGate that a device's traffic flows through, which is often an ISFW FortiGate, rather than the Upstream FortiGate. Information about the FortiClient device's registration and on-net status will appear only on the FortiGate that applies the FortiClient profile.

For more information about FortiClient profiles, see the Security Profiles handbook.

## FortiClient EMS

FortiClient Enterprise Management Server (FortiClient EMS) is a security management solution that enables scalable and centralized management of multiple endpoint devices. It can be used in a security fabric to provide visibility across the network, to securely share information and assign security profiles to endpoints.

For more information, refer to the FortiClient EMS documentation.

# Extended Devices

The following Fortinet products can be used to extend the use and range of a Security Fabric:

- FortiSwitch
- FortiAP
- FortiSandbox
- FortiMail, FortiWeb, and FortiCache

## FortiSwitch

A FortiSwitch can be added to a security fabric when it is managed by a FortiGate within the fabric, connecting to an interface that uses FortiTelemetry. Devices connected to the FortiSwitch will appear in the Security Fabric FortiView dashboard and security features, such as FortiClient profiles, will be applied to them.

For more information, see Managing FortiSwitches using FortiGate.

## FortiAP

FortiAPs can be added to extend a security fabric to your wireless devices. Devices connected to the FortiAP will appear in the Security Fabric FortiView dashboard. Ideally FortiClient should be installed on them to truly extend the security fabric to all of your devices. This also allows you to apply features, such as FortiClient profiles to them.

## FortiSandbox

Add FortiSandbox to your Security Fabric to improve security with sandbox inspection. The sandbox integration added in FortioS 5.4 allows FortiGates in the fabric to automatically receive signature updates from FortiSandbox and add the originating URL of any malicious file to a blocked URL list. FortiSandbox also integrates with FortiClient, allowed extended scanning to used by FortiClient devices.

For more information, see the Sandbox Inspection handbook.

## FortiMail, FortiWeb, and FortiCache

External Security Devices can be added to a Security Fabric to offload processes to other devices, such as a FortiWeb, FortiCache, or FortiMail. Example processes could include HTTP inspection, web caching, and anti- spam.

## Offloading HTTP traffic to FortiWeb

Use the following steps to offload HTTP traffic to FortiWeb to apply Web Application Firewall features to the traffic. Using these steps you can select the HTTP traffic to offload by adding a web application firewall profile configured for external inspection to selected firewall policies. Only the HTTP traffic accepted by those firewall policies is offloaded.

If you offload HTTP traffic to FortiWeb you can also apply other HTTP inspection to it from your FortiGate including virus scanning and web filtering.

A single FortiGate cannot offload HTTP traffic to both FortiCache and FortiWeb.

To offload HTTP traffic to FortiWeb:

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Feature Select** and turn on **Web Application Firewall**.
3. Go to **System > Cooperative Security Fabric**, enable **HTTP Service**, select **FortiWeb** and add the IP addresses of your FortiWeb devices. You can also select **Authentication** add a **password** if required.
4. Go to **Security Profiles > Web Application Firewall** and add or edit a Web Application Firewall profile and set **Inspection Device** to **External**.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a firewall policy, select **Web Application Firewall**, and select the profile that you set to use the external inspection device.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 51
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that
       communicates with the FortiWeb)
   set group address 0.0.0.0
   set server-list 5.5.5.25 255.255.255.255 (the IP address of the FortiWeb)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
end
```

## Offloading HTTP traffic to FortiCache

To offload Web Caching to FortiCache a FortiGate must support WAN Optimization and WAN Optimization must be enabled. For some FortiGate models you need to turn off disk logging to support WAN Optimization. See WAN Optimization in What's New for details.

Use the following steps to offload web caching to FortiCache. Using these steps you can select the web traffic to offload by selecting web caching in firewall policies. Only the web traffic accepted by those firewall policies will be offloaded.

A single FortiGate cannot offload HTTP traffic to both FortiCache and FortiWeb.

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Advanced > Disk Settings** and assign at least one disk to **WAN Optimization**.
3. Go to **System > Feature Select** and turn on **WAN Opt. & Cache**.

4. Go to **System > Cooperative Security Fabric**, enable **HTTP Service**, select **FortiCache** and add the IP addresses of your FortiCache devices. You can also select **Authentication** add a **password** if required.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a firewall policy and select **Web Cache**.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 51
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that
       communicates with the FortiCache)
   set group address 0.0.0.0
   set server-list 5.5.5.45 255.255.255.255 (the IP address of the FortiCache)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
end
```

## Offloading SMTP traffic to FortiMail

Use the following steps to offload SMTP traffic to FortiMail to apply FortiMail features to the traffic. Using these steps you can select the SMTP traffic to offload by adding an AntiSpam profile configured for external inspection to selected firewall policies. Only the SMTP traffic accepted by those firewall policies is offloaded.

If you offload HTTP traffic to FortiWeb you can also apply other HTTP inspection to it from your FortiGate including virus scanning and web filtering.

To be able to offload Anti-Spam processing to a FortiMail device you should:

1. Go to the **System Information** dashboard widget and make sure **Inspection Mode** is set to **Proxy-based**.
2. Go to **System > Feature Select** and turn on **Anti-Spam Filter**.
3. Go to **System > Cooperative Security Fabric**, enable **SMTP Service - FortiMail** and add the IP address of your FortiMail devices. You can also select **Authentication** add a **password** if required.
4. Go to **Security Profiles > Anti-Spam** and edit an Anti-Spam profile and set **Inspection Device** to **External**.
5. Go to **Policy & Objects > IPv4 Policy**, add or edit a Firewall policy, enable **Anti-Spam** and select the profile for which you set Inspection Device to External.

These steps add the following configuration to the CLI:

```
config system wccp
   set service-id 52
   set router-id 5.5.5.5 (the IP address of the FortiGate interface that
       communicates with the FortiMail)
   set group address 0.0.0.0
   set server-list 5.5.5.65 255.255.255.255 (the IP address of the FortiMail)
   set authentication enable
   set forward-method GRE
   set return-method GRE
   set assignment-method HASH
   set password *
end
```

FORTINET®

*High Performance Network Security*